

	COMPUTERS	Operations Order 5.3.00
	PHOENIX POLICE DEPARTMENT	Rev. 08/22 PAGE 1

1. **RESPONSIBILITIES**

A. Information Technology Bureau (ITB)	• Computer consulting • Technical support • Training assistance • Application development within the Department
B. User Bureau and Precincts	• Justifying, budgeting, operating, and maintaining microcomputer resources
C. User	• Training and use of specialized non-standard equipment or software packages

2. **ACQUISITION OF COMPUTER EQUIPMENT AND SOFTWARE**

A. Bureaus and Precincts - Each bureau or precinct with an information processing requirement they believe may be satisfied through the use of computer hardware or software, needs to:

- (1) Submit a proposal to ITB outlining the requirement and the expected benefits to be gained.
 - The purpose of the proposal is to obtain:
 - * A technical review of the proposal.
 - * A suggested configuration.
 - * A cost estimate.
- (2) Follow established Department procedures to obtain budget approval based on costs provided by ITB.
- (3) Provide a copy of ITB's technical review and the pertinent budget request to the Fiscal Management Bureau (FMB).

B. Fiscal Management Bureau Responsibilities

- (1) Ensure all budget submissions and purchase requests involving computer equipment or software are supported by an ITB technical review.
- (2) Route a copy of the purchase documentation for all computer software purchases to ITB to comply with [Administrative Regulation \(AR\) 1.86](#).
 - (a) A copy of the dated sales receipt or invoice is preferred for purchase documentation however any purchase documentation submitted must contain:
 - Vendor name
 - Software package purchased
 - Purchase date
 - Purchase price
 - (b) If these documents are not available, a copy of the Purchase Order Originating Report, Departmental Purchase Order, or Petty Cash Receipt will be routed to ITB.
- (3) In case of any external audit, FMB and City Accounts Payable will assist in the audit process by tracking the vouchers payable associated with Purchase Orders and Departmental Purchase Orders to the appropriate canceled checks held by City Accounts Payable.

	COMPUTERS	Operations Order 5.3.00
	PHOENIX POLICE DEPARTMENT	Rev. 08/22 PAGE 2

2. C. Information Technology Bureau - Will be responsible for the following tasks in the acquisition process:

- (1) Reviewing user requirements to determine those that can be effectively satisfied through computer hardware and software acquisitions.
- (2) Determining the technical and operational feasibility and providing the user with recommendations for system configuration and a cost breakdown.
- (3) Ensuring the proposed systems comply with City and Department guidelines regarding the use of standardized system components to ensure connectivity, compatibility, and a standard approach to applications.
- (4) Ensuring adequate justification exists if non-standard system components are proposed and/or recommended.
 - If non-standard components are required, ensure the user is aware of their increased responsibility for training and operation of the system and the potential lack of ITB support.
- (5) Assisting users in the preparation of purchase documentation in compliance with City regulations.
- (6) Providing assistance and recommendations to Department users concerning replacement and/or upgrade of existing hardware and software.

3. **SYSTEM INSTALLATION**

A. Responsibility - ITB will perform initial system installation including the installation and configuration of software packages.

B. Computer Documentation

(1) General Information

- (a) ITB will complete and submit any required licensing agreements or warranty registration material.
- (b) The components of all purchased software packages will be handled to comply with [AR 1.86](#).
- (c) Only properly obtained, authorized copies of software will be installed on Department computer systems.
- (d) Information on each purchased software package will be entered into a tracking database maintained by ITB.
- (e) Upon installing or adding equipment to a Department network, ITB will document and provide each participating user with appropriate operating procedures for their participation in the network.

(2) Personally Owned Software/Shareware

- (a) Any public domain, shareware, or personally purchased software must be pre-approved by ITB before its installation and appropriate user fees must be paid for the use of shareware products.
- (b) The user is solely responsible for all training, troubleshooting, and/or maintenance required to operate such software.

	COMPUTERS	Operations Order 5.3.00
	PHOENIX POLICE DEPARTMENT	Rev. 08/22 PAGE 3

3. B. (3) Maintenance of Documentation - Computer documentation will be maintained as follows:

(a) ITB	• A physical copy of the completed registration form • The original software licensing agreement • The original software distribution diskettes or media • A copy of the purchase documentation
(b) Bureau/Precinct	• Original software manuals, templates, and any other materials

4. TRAINING

A. Initial Training

- (1) ITB will provide initial familiarization training on new equipment and standard software packages to key users within the acquiring organization.
- (2) Training required for non-standard systems or software is the responsibility of the user.

B. Additional Training

- (1) In-depth proficiency in the use of computer products is normally acquired through practice and through reference to user documentation manuals.
- (2) Additional assistance may be available through ITB, the City MIS-sponsored computer training classes, or through commercially available training classes and packages.

5. APPLICATION DEVELOPMENT

A. ITB Responsibilities	• Provide primary program development support for database applications within the Department. • Provide spreadsheet templates for common applications that are required by multiple users. • Provide application troubleshooting support to user organizations on a time-available basis. • Publish and maintain a catalog of all computer applications used within the Department and coordinate new developments to promote standardization of common requirements where possible. • Monitor new developments to ensure computer applications are properly designed and coordinated with present and future requirements for centralized processing systems, such as the Computer Aided Dispatch (CAD) and the records management system (RMS)
B. User Bureau and Precinct Responsibilities	• Assist in the development, modification, and maintenance of database applications. • Provide primary programming support for spreadsheet and graphics applications. • Coordinate any new applications with ITB to ensure identical or similar systems do not already exist within the Department. • Provide necessary program descriptions to maintain a centralized applications catalog.

6. SYSTEM OPERATION

- A. System Managers - Bureaus/precincts with computers will appoint a system manager to serve as the primary point of contact between the user and ITB.

- (1) The system manager will monitor the day-to-day operations of their system.

	COMPUTERS	Operations Order 5.3.00
	PHOENIX POLICE DEPARTMENT	Rev. 08/22 PAGE 4

6. A. (2) The manager should possess a thorough understanding of the system and its operation.
 - (a) The manager should be capable of diagnosing and correcting routine system or program problems, training users, and assisting in the development or modification of applications.
 - (b) This individual is the key to effective use of computers within the Department.
- (3) The system managers will act as software custodians of the system.

B. Bureau/Precinct Responsibilities

- (1) Establish procedures to control access to computer resources and ensure only authorized personnel and programs are permitted on Department-owned systems.
- (2) Establish procedures to comply with security and privacy laws if personal or criminal history information is being stored and accessed on computer systems.
 - Questions regarding the applicability of security and privacy laws should be referred to the Records and Identification Bureau (R&I), or the Legal Unit.
- (3) Perform regular back-up of program and data files to minimize loss of information in the event of processing error or system failure.
- (4) Have all Department personnel using or otherwise operating Department computer equipment sign a copy of the [Employee Software and Internet Use Agreement](#) pertaining to software copying, installation, alteration and manipulation.
 - (a) Employees will receive a copy of the form during their orientation process.
 - (b) The employee and the employee's immediate supervisor will sign this document.
 - (c) A signed copy will be returned to the employee and the signed original will be placed in the employee's permanent personnel file.

7. **SYSTEM MAINTENANCE**

A. Bureau/Precinct Responsibilities

- (1) Bureaus/precincts with computers will establish procedures to perform routine first-level preventive maintenance procedures in computer equipment which should include:
 - Keeping equipment clean.
 - Not placing food or liquid on equipment.
 - Periodic cleaning of air filters.
 - Proper handling and storage of diskettes and tapes.
 - Periodic cleaning of disk and tape drives.
- (2) Bureaus/precincts will contact ITB in the event of system or component failure that cannot be diagnosed or corrected by the system manager.

B. ITB Responsibilities

- (1) Provide hardware repair support and maintenance assistance to bureaus/precincts in resolving system problems.
- (2) Provide assistance and orientation in development of proper preventive maintenance.

	COMPUTERS	Operations Order 5.3.00
	PHOENIX POLICE DEPARTMENT	Rev. 08/22 PAGE 5

7. B. (3) Conduct an annual audit of all systems to check for compliance with security requirements, including passwords, access codes, and access violations.

8. **DISTRIBUTION OF USER-DEVELOPED APPLICATIONS**

- A. Bureau/Precinct Responsibilities - Bureau and precincts developing database, spreadsheet, or word processing applications for potential Department-wide use will submit database programs and structures and/or word processing or spreadsheet macros to ITB prior to distributing these applications throughout the Department.

- B. Information Technology Bureau Responsibilities

- (1) Review the software to ensure Department-wide compatibility and inform the software developer of any modifications required based on the review.
- (2) Create and maintain a central repository of certified compatible computer software applications for Department-wide distribution.

9. **USE OF PERSONALLY OWNED COMPUTERS/SOFTWARE**

- A. General Guidelines - Employees will follow the listed guidelines when using a personally owned computer to accomplish employment specific work.

- (1) Employees will not be allowed to connect their computers to any Department-owned computer resources such as, but not limited to, Local Area Networks (LAN), printers, communications devices, or backup devices.
- (2) Employees will be able to provide the same level of ownership documentation on all software products installed on their computer as required in [AR 1.86](#) and paragraph 3 of this order.
 - Use of a personally owned computer to do employment-specific work with illegally acquired software could place liability for use of the illegal software on the City.

- B. Use of Personally Owned Computer Software - Use of personally owned computer software by Department employees on Department-owned computers to accomplish employment specific work will be governed by the following guidelines:

- (1) Employees will not be allowed to install or use personally owned computer software on Department-owned computers.
 - If a need can be shown that can only be met by a non-standard software product, ITB will authorize the purchase of that software product.
- (2) Employees will be allowed to use software that has been donated to the City or Department after the donated software has been submitted to ITB for approval for Department use.

10. **INTERNET/ELECTRONIC MAIL ACCESS**

- A. Responsibilities

- (1) All bureaus/precincts are responsible for continuous evaluation and monitoring of their internal Internet access accounts to ensure compliance with this order.

	COMPUTERS	Operations Order 5.3.00
	PHOENIX POLICE DEPARTMENT	Rev. 08/22 PAGE 6

10. A. (1) (a) All computer users are required to read and sign the [Employee Software and Internet User Agreement 5.3.A](#) and a copy of the document will be placed in the employee's personnel file.

- (b) If the employee refuses to sign [Employee Software and Internet User Agreement 5.3.A.](#), "refused" will be written on the employee's signature line and a copy will be placed in the employee's personnel file

- (2) ITB is responsible for assisting and supporting bureaus/precincts in fulfilling their responsibility.

- (3) Employees will access their work electronic mail at least once every shift and respond appropriately to written communications through email in a timely manner.

B. Internet Use

- (1) Internet access will only be used for job-related business/research.

- (2) Supervisors will monitor employees' use of the internet to ensure it is being used properly.

- (3) Department employees are prohibited from accessing any fee-based service unless authorized by their assistant chief.

- (4) Internet access and email are intended for work related research, data acquisition from professional and technical resources, data sharing with other criminal justice agencies, and acquiring approved products and services needed in the normal course of City business.

- Harassment or discrimination in any form will not be tolerated.

- (5) Employees utilizing the Internet to investigate criminal activity may be authorized to access chat rooms, bulletin boards, gambling, and adult sites that are off limits to all other Department Internet users.

C. Public Records

- (1) The City provides no assurance of privacy or confidentiality with respect to use of its electronic communications system.

- Email **will not** be used to send confidential or sensitive material.

- (2) Employees should be aware that information generated on, or handled by, electronic communications systems is subject to disclosure under the Arizona Public Records Act.

- The public can request copies of anything sent on email or accessed on the Internet on City equipment, including messages considered to be of a private or personal nature.
- Public requests received by the Department for email will be handled in accordance with [Operations Order 5.5.00, Release of Records](#).

D. Security Requirements

- (1) Close all active sessions before signing on to the Internet when accessing the Internet from a networked workstation.

- (2) Do not leave a workstation unattended during an active Internet session.

- (3) Because of security risks to Department systems, access to private email, Instant Messaging Systems, and chat rooms is prohibited.

	COMPUTERS	Operations Order 5.3.00
	PHOENIX POLICE DEPARTMENT	Rev. 08/22 PAGE 7

- Private email and instant messaging systems are defined as privately or commercially owned systems as opposed to City-sponsored systems.
- 10. D. (4) Only commercial software from a known source will be allowed for use on Department systems.
- (5) Shareware/freeware will not be allowed.
- (6) No employee may move to or run any downloaded executable on any Department-owned computer without the approval and assistance of ITB.
- (7) Downloading files larger than 10 megabytes must be coordinated with ITB to avoid impairing network response times.
- (8) Employees will not alter or manipulate any software on Department owned computers.
- (9) Passwords must be at least eight characters.
- (10) Passwords cannot be a word as listed in the dictionary or a proper name.
 - Modified spelling of words listed in the dictionary is acceptable.
- (11) Passwords must be changed every 60 days.
- (12) Passwords must contain at least one letter and one number or punctuation mark.
- (13) Passwords should not be reused.

11. **ACCESS TO REMOTE COMPUTING RESOURCES**

A. Department-Owned Computers

- (1) Department employees will be required to show an operational necessity to connect to a remote computer resource.
- (2) Department employees will not connect to a remote computing resource from any Department-owned computer concurrently connected to a Department LAN.
 - (a) National Crime Information Center (NCIC) security restrictions require any such connectivity be accomplished only if the computer has no physical connection to the Department's LAN resources.
 - (b) This can be accomplished by use of an isolation switch that physically disconnects the computer from the LAN when it is connecting via modem to a remote computing resource, or by connecting to remote computing resources via a computer that is not attached to a Department LAN.
 - (c) ITB should be contacted to assist in the configuration of the computer in either case.

B. Personally Owned Computers

- (1) Department employees using a personally owned computer system as a terminal to any external communications service will not use this computer for this purpose if it contains any Department-specific sensitive information on its internal mass storage system (hard drive).
- (2) External communications services include, but are not limited to, the Internet, America On-Line, Prodigy, CompuServe, or any other electronic mail or messaging service.

	COMPUTERS	Operations Order 5.3.00
	PHOENIX POLICE DEPARTMENT Rev. 08/22	PAGE 8

12. COMPUTER VIRUS PROTECTION

A. ITB Responsibilities	- Identify and purchase computer virus protection software for use on each LAN installation in the Department - Install and upgrade such software on Department LAN workstations and servers as required.
B. User Bureau/Precinct Responsibilities	Ensure that virus protection software is running whenever required workstations and servers are operating to check for files that may have been infected by a virus and to prevent any virus infections from occurring.

13. ELECTRONIC MAIL RETENTION POLICY - In order to comply with City requirements established by [AR 1.63](#) and City Manager's Letter 1175 involving retention of electronic mail, the listed Department procedures will be followed:

A. Information Technology Bureau will:

- (1) Run a CLEAN-UP process every two weeks which will search all Microsoft Mail users' **Sent Mail** and **Deleted Mail/Wastebasket** folders and automatically delete any messages in these folders.
 - Messages left in the INBOX will not be touched.
- (2) Retain tape backups of post office files to meet a 30-day retention requirement.

B. Microsoft Mail Users - Will be required to set a specific option in Microsoft Mail software in MAIL/OPTIONS selection; the EMPTY DELETED MAIL FOLDER WHEN EXITING option should not be checked.

- (1) This will allow the CLEAN-UP process to delete mail messages after they have been backed up for retention.
- (2) For Microsoft Mail for Windows users, these messages may be deleted from SENT MAIL or INBOX folders but may not be deleted from DELETED MAIL/WASTEBASKET folder.

14. SECURITY SYSTEM BREACHES

A. Definitions

- (1) Breach - An unauthorized acquisition of an access to unencrypted or un-redacted computerized data that materially compromises the security or confidentiality of personal information maintained by the Department as part of a database of personal information regarding multiple individuals which causes or is reasonably likely to cause substantial economic loss to an individual.
- (2) Encrypted - Use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without use of a confidential process or key.
- (3) Personal Information - Includes an individual's first name, or first initial and last name, in combination with the individual's social security number, driver's license number, financial account number, or credit or debit account number.

B. Procedures

- (1) If it is determined a security system (unencrypted computerized data) has been breached, ITB will notify the individuals affected.

	COMPUTERS	Operations Order 5.3.00
	PHOENIX POLICE DEPARTMENT	Rev. 08/22 PAGE 9

14. B. (2) Individuals will be notified by one of the following notification processes:

- Written notification
- Electronic notification
- Telephonic notification

(3) Notice will be made to the affected individuals without unreasonable delay.

EXCEPTION: Notification may be delayed if it is determined notification will impede a criminal investigation.

Last Organizational Review: